Virtual Private Networks (VPN) MacWorld/Pro Conference VPN Buyers Guide

Bill Vlahos
Network Services Engineer
OAO Corporation contracted to Jet Propulsion Laboratory
July 22, 1999

Objectives

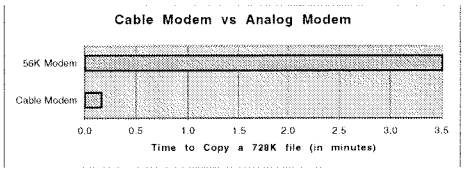
- What is Remote Access?
- What is a VPN?
- Why do I want it?
- How do I choose it?
- When can I use it?
- Opportunities to lead using Macs
  - Most common VPN is Microsoft's built-in

Introduction to Remote Access

- Current situation
  - Dial up 56k v.90 or 128k ISDN
    - Multi-protocol
  - IP via Internet
    - IP only
    - IP address restriction on web & ftp servers
    - Clear text with little encryption

Technology Direction

- WEB and FTP information dissemination everywhere
- ISP services commonplace (with features you can't provide)
  - High Speed Internet services available
  - Wireless Internet access
  - International ISP services available
- Corporate business on web
  - Timecards
  - Order processing
- Off-site people
  - Telecommuters
  - Customers
  - Contractors



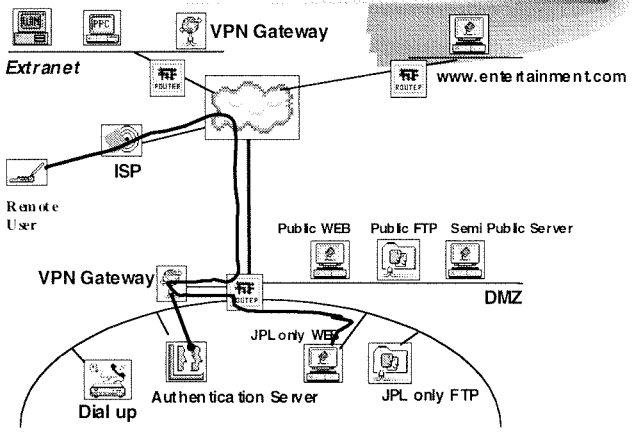
What is a VPN?

High-speed, secure, controlled connections from anywhere!

- Three forms
  - Client to server
    - Software solution plus authentication (often local)
  - Client to network (gateway)
    - Client software gateway software or hardware plus authentication server
  - Network to network (Gateway-gateway or LAN-LAN)
    - Hardware solution for stability and performance

VPN Design Overview

Client-server, Client-gateway, LAN-LAN



Which type of VPN?

- Client-server
  - Complete encryption end to end
  - Doesn't scale easily/how do you authenticate users
  - Performance and security issues
- Client-network
  - High performance
  - Scalable (can leverage existing infrastructure)
  - Requires client software
- Network-network
  - No client requirements (support all platforms)
  - Doesn't go everywhere

The 3 Components of a VPN Focus on Client-network

- VPN Gateway
  - External interface (IPSec only)
  - Internal interface (multi-protocol inside Company network)
- Authentication Server
- Client software

Features & Options

- Authentication Servers
  - RADIUS
  - TACACS
  - SecureID Card
  - PKI
- Type of Gateway
  - Appliance Box
  - Software application
- Performance Expectations
  - Simultaneous connections
  - Network throughput
- Standards
  - PPTP (Microsoft)
  - L2TP (Microsoft & Cisco)
  - IPSec (Ratified standard)
- Services
  - IP
  - AppleTalk
  - IPX
  - NAT (Network Address Translation)
  - Encryption levels (DES, 3DES, etc)

Macintosh Supported Vendors

Vendor (Alphabetical)	IKE	IPSec	RADIUS	Form	Cross vendor support
AltaVista Tunnel/Compaq	No	No	No	S/W	Unsure
Bay Networks/NorTel	No	No	Yes	Box	Uses NTS client
Cisco Systems	Yes	Yes	?	Both	Uses Network Associates client
Compatible Systems	Yes	Yes	Yes	Box	Gateways some, clients limited
InfoExpress	Yes	No*	Yes	S/W	No
iPass	No	No	No	N/A	No
Microsoft	No	No	No	S/W	Can use NTS client
Network Associates(PGPnet)	Yes	Yes	No	S/W	Yes
PGPnet from MIT (Freeware)	Yes	Yes	No	S/W	Yes
Network TeleSystems(NTS)	No	No	Yes	Both	Yes
Novell	No	No	Yes	s/w	No
TimeStep	Yes	Yes	No*	Box	Some
V-ONE	Yes	No	Yes	S/W	

**Planned*

Contacting Vendors

AltaVista Tunnel /Compaq http://altavista.software.digital.com/tunnel/
Bay Networks/NorTel http://www.nortelnetworks.com
Cisco Systems http:// www.cisco.com
Compatible Systems http:// www.compatible.com
InfoExpress http:// www.infoexpress.com
*iPass http://www.centralhouse.com/ipass/service_overview.html
Network Associates(PGPnet) http://www.nai.com/
PGPnet from MIT (Freeware) http://web.mit.edu/network/pgp.html
Network TeleSystems(NTS) http://www.nts.com/
*Novell http://www.valuemedia.com/value/pages/009325.html
TimeStep http:// www.timestep.com
V-ONE http//www.v-one.com/smartgate.htm

Authentication Servers

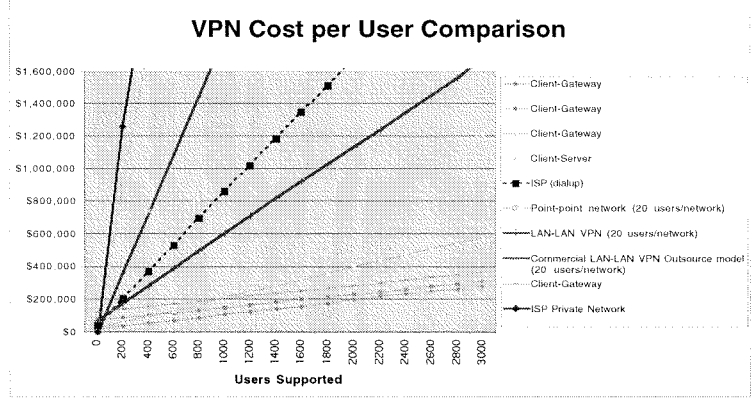
- MacRADIUS http://www.cyno.com
  - IETF Standards based RADIUS (Remote Authentication Dial-in User Service) server with extensive AppleScript support.
- HandyTACACS http://www.arithmetica.ch/HandyTacacs/index.shtml
  - TACACS (Terminal Access Controller Access Control System)
- Accounts on the Gateway
  - Not scalable
- Public Key Infrastructure (PKI) - not Mac based
  - Entust http://www.entrust.com/
  - Versign http://www.verisign.com/
  - x.509 Certificates

Sample Requirements for VPNs

your mileage may vary

- **Encryption (IPSec)**
- **smart tunnel (appropriate use)**
- **NAT (Network Address Translation)**
- **log source and NAT IP addresses**
- log traffic indicator
- **RADIUS**
- IKE/PKI Entrust (in future)
- Y2K
- Encryption key rotation
- IP
- AppleTalk
- IPX
- failover & redundancy
- Connectivity (Client-gateway, gateway-gateway, gateway at edge of JPL network)
- **Mac**, Win95/98/NT
- **client s/w exportable**
- **application independent**
- 500 simultaneous connections
- 27 Mb/s throughput
- load balancing
- password protected
- Console port protected
- passwords changeable
- SNMP monitoring
- vendor replacement

Cost per user for 3 years



Client-Gateway VPN

- Advantages
  - All network services automatically protected
  - Ubiquitous Internet access
  - ISP & technology independent
  - Traffic is encrypted before it leaves computer
  - User is authenticated at connection time
  - Smart tunnel feature assures "appropriate usage"
  - Standards based (IPSec)
  - Leverage current infrastructure (authentication, etc.)
  - No changes to existing services
- Disadvantages
  - Software installed on remote client computer

Gateway-Gateway VPN

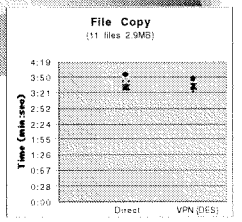
- Advantages
  - Does not require client installs on remote computers
  - Supports all computer platforms
  - ISP independent. Gateway(s) can be anywhere on the Internet
  - Smart tunnel feature assures "appropriate usage"
  - "Always-on" connection
- Disadvantages
  - Difficult to control who is on the remote network

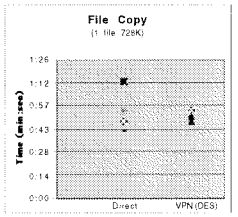
So does it work?

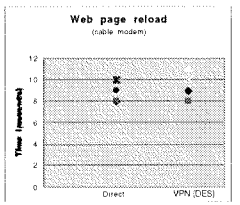
- Yes!
- How well do you ask?...

VPN Performance Impact
High-speed cable modem

- **We expected to see some degradation but did not find any.**

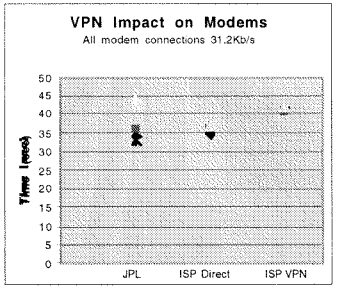


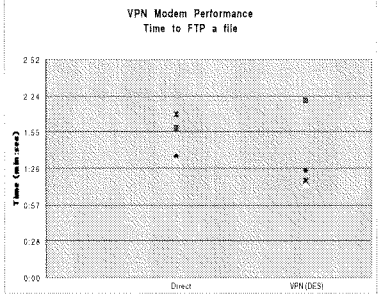




VPN Performance Impact Analog Modems

- **Good line conditions**
  Small penalty (17%)
- **Poor line conditions**
  No consistent penalty





Challenges for deployment

- Remote site firewalls
- Support of computers owned by other institutions
- Who will support outside users
- IPSec ratified Nov. '98. Will take time to stabilize
- Cross-vendor compatibility not good

Additional Information

- IPSecurity (IPSec) RFC 2409 (IKE {Internet Key Exchange}) and RFC 2407 (ISAKMP {Internet Security Association and Key Management Protocol}). http://www.ietf.org/html.charters/ipsec-charter.html
- RADIUS (Remote Authentication Dial In User Service) RFC 2058 (Authentication) and RFC 2059 (Accounting)
- My email address: bvlahos@jpl.nasa.gov

Demo

Q & A

Thank you